Appl. No. 09/622,047
Reply to Office Action of October 19, 2005

Attorney Docket: P65855US0

Amendments to the Claims:

The listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

Claim 1 (previously presented): A method for block encryption of discrete data, comprising the steps of: generating an encryption key in the form of a set of subkeys, breaking down a data block into $N \geq 2$ subblocks and alternately converting said subblocks by performing a two-place operation on the subblock and the subkey, wherein, prior to carrying out said two-place operation on i-th subblock and subkey, a substitution operation is performed on the subkey depending on j-th subblock, where $i \neq j$.

Claim 2 (previously presented): The method according to claim 1, wherein an operation of permuting subkey bits depending on the j-th subblock is used as the j-th subblock-dependent substitution operation.

Claim 3 (currently amended): The method according to claim 2, wherein an operation of cyclic offsetting subkey bits depending on the j-th subblock is used as the j-th subblock-dependent operation of permuting subkey ~~subket~~ bits.

Claim 4 (cancelled)